セキュリティ サービスの設定

この章で説明する内容は、次のとおりです。

セキュリティ サービスの設定の概要

Secure Web Applianceは、セキュリティ コンポーネントを使用してさまざまなマルウェアの脅威からエンド ユーザを保護します。グループ ポリシーごとにマルウェア対策と Web レピュテーション設定値を設定できます。アクセス ポリシーを設定すると、AsyncOS for Web はブロックするコンテンツを判定するときに、マルウェア対策スキャンと Web レピュテーション スコアの組み合わせを使用することを選択できるようになります。

マルウェアからエンドユーザーを保護するには、アプライアンスでこれらの機能をイネーブルにしてから、ポリシーごとにマルウェア対策と Web レピュテーションの設定値を設定します。

オプション	説明	リンク
マルウェア対策スキャン（Anti-malware scanning）	アプライアンスに統合された複数のマルウェア対策スキャン エンジンを使用して、マルウェアの脅威をブロックします。	マルウェア対策スキャンの概要 （5 ページ）

オプション	説明	リンク
Web レピュテーション フィルタ（Web Reputation Filters）	Web サーバーの動作を分析し、URL に URL ベースのマルウェアが含まれているかどうかを判定します。	Web レピュテーション フィルタの概要 （2 ページ）
Secure Endpoint	ファイル レピュテーションを評価し、ファイルの特性を分析することによって、ダウンロードファイルに潜む脅威から保護します。	ファイル レピュテーション フィルタリングとファイル分析の概要

関連項目

- マルウェア対策とレピュテーション フィルタの有効化 （9 ページ）
- 適応型スキャンについて （8 ページ）

Web レピュテーション フィルタの概要

Web レピュテーション フィルタは、Web ベースのレピュテーション スコア（WBRS）を URL に割り当て、URL ベースのマルウェアが含まれている可能性を判断します。 Secure Web Appliance は、Web レピュテーション スコアを使用して、未然にマルウェア攻撃を特定して防ぎます。Web レピュテーション フィルタは、アクセス、復号化、および Cisco データ セキュリティの各ポリシーで使用できます。

Web レピュテーション スコア

Web レピュテーション フィルタでは、データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在

- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

（注） シスコは、ユーザー名、パスフレーズ、クライアント IP アドレスなどの識別情報を収集しません。

Web レピュテーション フィルタの動作のしくみについて

Web レピュテーション スコアは URL 要求に対して実行されるアクションに関連付けられます。各ポリシー グループを設定して、特定の Web レピュテーション スコアにアクションを関連付けることができます。使用可能なアクションは、URL 要求に割り当てられているポリシー グループのタイプによって異なります。

ポリシー タイプ	操作
アクセス ポリシー（**Access Policies**）	ブロック、スキャン、または許可から選択できます。
復号化ポリシー（**Decryption Policies**）	ドロップ、復号化、またはパススルーから選択できます。
シスコ データ セキュリティ ポリシー（**Cisco Data Security Policies**）	ブロックまたはモニターから選択できます。

アクセス ポリシーの Web レピュテーション

アクセス ポリシーに Web レピュテーションを設定する場合は、手動で設定するか、AsyncOS for Web で適応型スキャンを使用して最適なオプションを選択することができます。適応型スキャンがイネーブルの場合は、各アクセス ポリシーで Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。

スコア	アクション	説明	例
-10 ～ -6.0	ブロック（Block）	不正なサイト。要求はブロックされ、以降のマルウェア スキャンは実行されません。	• URL がユーザーの許可なしに情報をダウンロード。 • URL ボリュームが急上昇。 • URL が人気のあるドメインの誤入力。

スコア	アクション	説明	例
-5.9 ～ 5.9	スキャン（Scan）	判別不能なサイト。さらにマルウェア スキャンを行うために、DVS エンジンに要求が渡されます。DVS エンジンは、要求とサーバー応答のコンテンツをスキャンします。	• 動的 IP アドレスを持ち、ダウンロード可能なコンテンツを含む最近作成された URL。 • Web レピュテーション スコアがプラスのネットワーク オーナーの IP アドレス。
6.0 ～ 10.0	許可（Allow）	正常なサイト。要求は許可されます。マルウェア スキャンは必要ありません。	• URL にダウンロード可能なコンテンツが含まれていない。 • 歴史が長く信頼できる大規模ドメイン。 • 複数の許可リストに記載されているドメイン。 • 評価が低い URL へのリンクがない。

デフォルトでは、+7 の Web レピュテーション スコアが割り当てられている HTTP 要求の URL は許可され、さらなるスキャンは必要ありません。しかし、+3 などの低いスコアの HTTP 要求は、マルウェアをスキャンする Cisco DVS エンジンに自動的に転送されます。レピュテーションが非常に低い HTTP 要求の URL はブロックされます。

関連項目

- 適応型スキャンについて （8 ページ）

復号化ポリシーの Web レピュテーション

スコア	アクション	説明
-10 ～ -9.0	削除（Drop）	不正なサイト。要求は、エンドユーザーへの通知なしでドロップされます。この設定の使用には注意が必要です。
-8.9 ～ 5.9	復号化（Decrypt）	判別不能なサイト。要求は許可されますが、接続が復号化され、アクセス ポリシーが復号化されたトラフィックに適用されます。
6.0 ～ 10.0	パススルー（Pass through）	正常なサイト。要求は、検査や復号化なしで渡されます。

Cisco データ セキュリティ ポリシーの Web レピュテーション

スコア	アクション	説明
-10 ～ -6.0	ブロック（Block）	不正なサイト。トランザクションはブロックされ、以降のスキャンは実行されません。
-5.9 ～ 0.0	モニター（Monitor）	トランザクションはWebレピュテーションに基づいてブロックされず、引き続きコンテンツ（ファイルタイプとサイズ）の検査が行われます。 （注）　スコアがないサイトはモニターされます。

マルウェア対策スキャンの概要

Secure Web Applianceのマルウェア対策機能は、Cisco DVS™ エンジンとマルウェア対策スキャンエンジンを併用して、Web ベースのマルウェアの脅威を阻止します。DVS エンジンは、Webroot™、McAfee、Sophos マルウェア対策スキャン エンジンと連携します。

スキャン エンジンはトランザクションを検査して、DVS エンジンに渡すマルウェア スキャンの判定を行います。DVSエンジンは、マルウェア スキャンの判定に基づいて、要求をモニターするかブロックするかを決定します。アプライアンスのアンチマルウェア コンポーネントを使用するには、マルウェア対策スキャンをイネーブルにして、グローバル設定値を設定してから、各種のポリシーに特定の設定を適用する必要があります。

関連項目

- マルウェア対策とレピュテーション フィルタの有効化 （9 ページ）
- 適応型スキャンについて （8 ページ）
- McAfee スキャン （7 ページ）

DVS エンジンの動作のしくみについて

DVS エンジンは、Web レピュテーション フィルタから転送された URL のトランザクションに対してマルウェア対策スキャンを実行します。Web レピュテーション フィルタは、特定の URL にマルウェアが含まれている可能性を計算し、URL スコアを割り当てます。このスコアは、トランザクションをブロック、スキャンまたは許可するアクションに関連付けられています。

割り当てられた Web レピュテーション スコアがトランザクションをスキャンすることを示している場合、DVS エンジンは URL 要求とサーバー応答のコンテンツを受信します。DVS エンジンはスキャン エンジン（Webroot および（または）Sophos、または McAfee）と連携して、マルウェア スキャンの判定を返します。DVS エンジンは、マルウェア スキャンの判定およびアクセス ポリシーの設定情報を使用して、クライアントへのコンテンツをブロックするか配信するかを判定します。

複数のマルウェア判定の使用

DVS エンジンは、1 つの URL に対して複数のマルウェア判定を下すことがあります。イネーブルなスキャン エンジンの一方または両方から複数の判定が返される場合もあります。

- **異なるスキャン エンジンによるさまざまな判定。**SophosまたはMcAfeeのどちらか一方とWebrootを同時にイネーブルにすると、それぞれのスキャン エンジンが同じオブジェクトに対して異なるマルウェア判定を返すことがあります。イネーブルな両方のスキャンエンジンから 1 つの URL に対して複数の判定が返された場合、アプライアンスは最も制限が厳しいアクションを実行します。たとえば、一方のスキャンエンジンがブロックの判定を返し、他方のスキャン エンジンがモニターの判定を返した場合、DVS エンジンは常に要求をブロックします。
- **同じスキャン エンジンからの異なる判定。**オブジェクトに複数の感染が含まれている場合、1 つのスキャン エンジンが 1 つのオブジェクトに対して複数の判定を返すことがあります。同じスキャン エンジンが 1 つの URL に対して複数の判定を返した場合、アプライアンスは最も優先順位の高い判定に従ってアクションを実行します。以下のリストは、可能性があるマルウェア スキャンの判定を優先順位が高いものから順に示しています。
- ウィルス
- トロイのダウンローダ
- トロイの木馬
- トロイのフィッシャ
- ハイジャッカー
- システム モニター
- 商用システム モニター
- ダイヤラ
- ワーム
- ブラウザ ヘルパー オブジェクト
- フィッシング URL
- アドウェア
- 暗号化ファイル
- スキャン不可
- その他のマルウェア

Webroot スキャン

Webrootスキャン エンジンはオブジェクトを検査してマルウェア スキャンの判定を行い、判定を DVS エンジンに送信します。Webroot スキャン エンジンは、以下のオブジェクトを検査します。

- **URL 要求。**Webroot は URL 要求を評価して、URL にマルウェアの疑いがあるかどうかを判別します。この URL からの応答にマルウェアが含まれている可能性があると Webroot が判断した場合、アプライアンスは、アプライアンス独自の設定に応じて、要求をモニターまたはブロックします。Webroot によって要求が正常である評価された場合、アプライアンスは URL を取得し、サーバーの応答をスキャンします。

- **サーバー応答。**アプライアンスがURLを取得すると、Webrootはサーバー応答のコンテンツをスキャンし、Webroot シグニチャ データベースと照合します。

McAfee スキャン

McAfee スキャン エンジンは、HTTP 応答内の Web サーバからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定をDVSエンジンに渡し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。

McAfee スキャン エンジンは以下の方法を使用して、マルウェア スキャンの判定を行います。

- ウィルス シグニチャ パターンの照合
- ヒューリスティック分析

ウィルス シグニチャ パターンの照合

McAfee は、そのデータベース内のウィルス定義をスキャン エンジンに使用し、特定のウィルスや各種のウィルスなどの潜在的に望ましくないソフトウェアを検出します。ファイル内のウィルス シグニチャを検索します。McAfee をイネーブルにした場合、McAfee スキャン エンジンはこの方法を使用して、サーバー応答のコンテンツをスキャンします。

ヒューリスティック分析

ヒューリスティック分析は、特定のルールではなく、一般的なルールを使用して新しいウィルスとマルウェアを検出する手法です。ヒューリスティック分析を使用する場合、McAfeeスキャン エンジンは、オブジェクトのコードを確認して一般的なルールを適用し、オブジェクトがどの程度ウィルスに類似しているかを判断します。

ヒューリスティック分析を使用すると、偽陽性（ウイルスと指摘された正常なコンテンツ）の報告が増加し、アプライアンスのパフォーマンスが影響を受ける可能性があります。McAfee をイネーブルにするときに、オブジェクトのスキャンでヒューリスティック分析をイネーブルにするかどうかを選択できます。

McAfee カテゴリ

McAfee の判定	**マルウェア スキャン判定カテゴリ**
既知のウィルス	ウィルス
トロイの木馬	トロイの木馬
ジョーク ファイル	アドウェア
テスト ファイル	ウィルス
ワナビ	ウィルス
不活化	ウィルス

McAfee の判定	マルウェア スキャン判定カテゴリ
商用アプリケーション	商用システム モニター
望ましくないオブジェクト	アドウェア
望ましくないソフトウェア パッケージ	アドウェア
暗号化ファイル	暗号化ファイル

Sophos スキャン

Sophos スキャン エンジンは、HTTP 応答内の Web サーバーからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニターするかブロックするかを決定できるようにします。McAfee アンチマルウェア ソフトウェアがインストールされているときに、McAfee スキャン エンジンではなく、Sophos スキャン エンジンをイネーブルにする必要がある場合があります。

適応型スキャンについて

アダプティブスキャン機能は、どのマルウェア対策スキャンエンジン（ダウンロードファイルの Secure Endpoint スキャンを含む）によって Web 要求を処理するかを決定します。

適応型スキャン機能は、スキャンエンジンを実行する前に、マルウェアとして特定するトランザクションに「アウトブレイク ヒューリスティック（Outbreak Heuristics）」マルウェア対策カテゴリを適用します。アプライアンスでマルウェア対策設定を行うときに、これらのトランザクションをブロックするかどうかを選択できます。

適応型スキャンとアクセス ポリシー

適応型スキャンをイネーブルにした場合は、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目の一部がやや異なります。

- 各アクセス ポリシーでは Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。
- 各アクセス ポリシーではマルウェア対策スキャンをイネーブルにできますが、どのマルウェア対策スキャンエンジンをイネーブルにするかは選択できません。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。

（注） 適応型スキャンがイネーブルになっておらず、アクセス ポリシーに Web レピュテーションとマルウェア対策の特定の設定項目が設定されている場合に、適応型スキャンをイネーブルにすると、既存の Web レピュテーションとマルウェア対策の設定が上書きされます。

ポリシーごとのSecure Endpointの設定は、適応型スキャンがイネーブルかどうかに関わらず同じです。

マルウェア対策とレピュテーション フィルタの有効化

始める前に

Web レピュテーションフィルタ、DVSエンジン、およびスキャンエンジン（Webroot、McAfee、Sophos）がイネーブルになっていることを確認します。デフォルトでは、システムのセットアップ時にこれらがイネーブルになります。

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 必要に応じて、以下の項目を設定します。

設定	説明
Web レピュテーション フィルタリング（Web Reputation Filtering）	Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。
適応型スキャン（Adaptive Scanning）	適応型スキャンをイネーブルにするかどうかを選択します。Web レピュテーション フィルタリングがイネーブルの場合にのみ、適応型スキャンをイネーブルにできます。
ファイル レピュテーション フィルタリングとファイル分析（File Reputation Filtering and File Analysis）	『ファイルレピュテーションと分析サービスの有効化と設定』を参照してください。
Secure Endpoint コンソールの統合（[詳細設定（Advanced）] > [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）]）	お使いのアプライアンスを Secure Endpoint コンソールと統合するには、[Secure Endpointコンソールでのアプライアンスの登録（Register the Appliance with Secure Endpoint AMP for Endpoints console）] をクリックします。詳細な手順については、Cisco Secure Endpoint AMP for Endpoints コンソールとアプライアンスの統合（17 ページ）を参照してください。

設定	説明
DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）	スキャン対象オブジェクト サイズの最大値を指定します。 指定した [最大オブジェクトサイズ（Maximum Object Size）] の値は、すべてのマルウェア対策とウイルス対策スキャン エンジンおよび Secure Endpoint 機能によってスキャンされる、要求と応答のサイズ全体に適用されます。これは、アーカイブ検査で検査可能なアーカイブの最大サイズも指定します。アーカイブ検査について詳しくは、アクセス ポリシー：オブジェクトのブロッキングを参照してください。 アップロードまたはダウンロードのサイズがこのサイズを超えると、セキュリティ コンポーネントは、進行中のスキャンを中断し、Web プロキシにスキャンの判定を提供しない可能性があります。検査可能なアーカイブがこのサイズを上回ると、[スキャンされていません（Not Scanned）] と示されます。
Sophos	Sophos スキャン エンジンをイネーブルにするかどうかを選択します。
McAfee	McAfee スキャン エンジンをイネーブルにするかどうかを選択します。 McAfee をイネーブルにするときに、ヒューリスティック スキャンをイネーブルにするかどうかも選択できます。 （注） ヒューリスティック分析はセキュリティ保護を向上させますが、偽陽性が生じてパフォーマンスが低下する可能性があります。
Webroot	Webroot スキャン エンジンをイネーブルにするかどうかを選択します。 Webroot スキャン エンジンをイネーブルにするときに、脅威リスクしきい値（TRT）を設定できます。TRT はマルウェアが存在する確率に対して数値を割り当てます。 独自のアルゴリズムによって URL 照合シーケンスの結果を評価し、脅威リスク レーティング（TRR）を割り当てます。この値は、TRT 設定に関連付けられます。TRR 値が TRT 以上の場合、URL はマルウェアと見なされ、さらなる処理に渡されます。 （注） 脅威リスクしきい値に 90 よりも低い値を設定すると、URL ブロッキング レートが劇的に増加し、正当な要求が拒否されてしまいます。TRT のデフォルト値 90 を維持することを強く推奨します。TRT 設定の最小値は 51 です。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- 適応型スキャンについて （8 ページ）
- McAfee スキャン （7 ページ）

Secure Endpoint サービスのキャッシュのクリア

Cisco Secure Endpoint キャッシュ消去機能は、クリーンなファイル、悪意のあるファイル、不明なファイルについて、ファイルレピュテーションの判定結果を消去します。

（注） Cisco Secure Endpoint キャッシュはパフォーマンス向上のために使用されます。**Clear Cache** コマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下する可能性があります。

ステップ 1 [セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [セキュアエンドポイントサービス（Secure Endpoint Services）] セクションで、[キャッシュ消去（Clear Cache）] をクリックし、動作を確認します。

ポリシーにおけるマルウェア対策およびレピュテーションの設定

[マルウェア対策およびレピュテーションフィルタ（Anti-Malware and Reputation Filters）] がアプライアンスでイネーブルの場合は、ポリシー グループでさまざまな設定値を設定できます。マルウェア スキャンの判定に基づいて、マルウェア カテゴリのモニターまたはブロックをイネーブルにできます。

以下のポリシー グループにマルウェア対策を設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（Access Policies）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定 （12 ページ）
発信マルウェア スキャン ポリシー（Outbound Malware Scanning Policies）	発信マルウェア スキャン ポリシーによるアップロード要求の制御

以下のポリシー グループに Web レピュテーションを設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（Access Policies）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定 （12 ページ）
復号化ポリシー（Decryption Policies）	復号化ポリシー グループの Web レピュテーション フィルタの設定 （16 ページ）

ポリシー タイプ	タスクへのリンク
シスコ データ セキュリティ ポリシー（**Cisco Data Security Policies**）	復号化ポリシー グループの Web レピュテーション フィルタの設定 （16 ページ）

アクセスポリシーでのみ Secure Endpoint 設定を構成できます。ファイル レピュテーションと分析機能の設定を参照してください

アクセスポリシーにおけるマルウェア対策およびレピュテーションの設定

適応型スキャンがイネーブルの場合、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目は、適応型スキャンがオフの場合とやや異なります。

（注） 展開にセキュリティ管理アプライアンスが含まれており、この機能をプライマリ構成で設定する場合、このページのオプションは、関連するプライマリ構成で適応型セキュリティが有効になっているかどうかに応じて異なります。[Web] > [ユーティリティ（Utilities）] > [セキュリティサービス表示（Security Services Display）] ページで、セキュリティ管理アプライアンスの設定を確認します。

- 適応型スキャンについて （8 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがイネーブルの場合）

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション設定（Web Reputation Settings）] セクションで、Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。適応型スキャンによって、各 Web 要求に最適な Web レピュテーション スコアのしきい値が選択されます。

ステップ 5 [セキュアエンドポイント設定（Secure Endpoint Settings）] セクションで設定項目を設定します。

ステップ 6 [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7 必要に応じて、ポリシーのマルウェア対策設定を指定します。

疑わしいユーザー エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、トラフィックをスキャンするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。 （注） FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザーエージェントとして検出されません。
マルウェア対策スキャンを有効にする（Enable Anti-Malware Scanning）	マルウェアのトラフィックをスキャンするために、DVS エンジンを使用するかどうかを選択します。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。 （注） [アウトブレイクヒューリスティック（Outbreak Heuristics）] カテゴリは、スキャンエンジンの実行前に適応型スキャンによってマルウェアとして識別されたトランザクションに適用されます。 （注） 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- 適応型スキャンについて （8 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがディセーブルの場合）

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション設定（Web Reputation Settings）] セクションで設定項目を設定します。

ステップ 5 [セキュアエンドポイント設定（Secure Endpoint Settings）] セクションで設定項目を設定します。

ステップ 6 [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7 必要に応じて、ポリシーのマルウェア対策設定を指定します。

（注） Webroot、Sophos、または McAfee スキャンをイネーブルにすると、このページの [マルウェア カテゴリ（Malware Categories）] で、追加のカテゴリをモニターするかブロックするかを選択できます。

設定	説明
疑わしいユーザー エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。 （注） FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザーエージェントとして検出されません。
Webroot を有効にする（Enable Webroot）	アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。
Sophos または McAfee を有効にする（Enable Sophos or McAfee）	アプライアンスがトラフィックをスキャンする際に、Sophos または McAfee スキャン エンジンを使用できるようにするかどうかを選択します。
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。このセクションに表示されるカテゴリは、上記でイネーブルにするスキャン エンジンによって異なります。

設定	説明
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。 （注） 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- アクセス ポリシーの Web レピュテーション スコアのしきい値の設定 （15 ページ）
- マルウェアのカテゴリについて （21 ページ）

Web レピュテーション スコアの設定

Secure Web Applianceをインストールして設定すると、Web レピュテーション スコアのデフォルト設定が指定されます。ただし、Web レピュテーション スコアのしきい値の設定は組織のニーズに合わせて変更できます。各ポリシー グループに応じた Web レピュテーション フィルタを設定してください。

アクセス ポリシーの Web レピュテーション スコアのしきい値の設定

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

ステップ 2 [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列で、編集するアクセス ポリシー グループのリンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがイネーブルになっていることを確認します。

ステップ 5 マーカーを動かして、URL のブロック、スキャン、許可の各アクションの範囲を変更します。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

（注） 適応型スキャンがディセーブルの場合は、アクセス ポリシーの Web レピュテーション スコアのしきい値を編集できます。

復号化ポリシー グループの Web レピュテーション フィルタの設定

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] を選択します。

ステップ 2 [Web レピュテーション（Web Reputation）] 列で、編集する復号化ポリシー グループのリンクをクリックします。

ステップ 3 [Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4 [Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがオンになっていることを確認します。

ステップ 5 マーカーを動かして、URL のドロップ、復号化、およびパススルー アクションの範囲を変更します。

ステップ 6 [スコアを持たないサイト（Sites with No Score）] フィールドで、Web レピュテーション スコアが割り当てられていないサイトの要求に対して実行するアクションを選択します。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

データ セキュリティ ポリシー グループの Web レピュテーション フィルタの設定

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [シスコ データ セキュリティ（Cisco Data Security）] を選択します。

ステップ 2 [Web レピュテーション（Web Reputation）] 列で、編集するデータ セキュリティ ポリシー グループのリンクをクリックします。

ステップ 3 [Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。

これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4 マーカーを動かして、URL のブロックおよびモニター アクションの範囲を変更します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

（注） Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

Cisco Secure Endpoint AMP for Endpoints コンソールとアプライアンスの統合

お使いのアプライアンスを Secure Endpoint コンソールと統合すると、 Secure Endpoint コンソールで以下の操作を実行できます。

- シンプル カスタム検出リストを作成する。
- シンプル カスタム検出リストに新しい悪意のあるファイル SHA を追加する。
- アプリケーション許可リストを作成する。
- アプリケーション許可トリストに新しいファイル SHA を追加する。
- カスタム ポリシーを作成する。
- カスタムポリシーにシンプルカスタム検出リストおよびアプリケーション許可リストを関連付ける。
- カスタム グループを作成する。
- カスタム グループにカスタム ポリシーを関連付ける。
- 登録済みのアプライアンスをデフォルトのグループからカスタム グループに移動する。
- 特定のファイル SHA のファイル トラジェクトリの詳細を表示する。

アプライアンスを Secure Endpoint コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。

統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバーから得られた判定は、Secure Endpoint コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。

ファイル SHA がすでにグローバルに悪意のあるものとしてマークされている場合、Secure Endpoint コンソールで同じファイル SHA をブロックリストに追加すると、ファイルの判定結果は「悪意のあるもの」になります。

[高度なマルウェア防御（Secure Endpoint）] レポートページには、新しいセクション、[カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] があります。このセクションには、Secure Endpoint コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションに [シンプルカスタム検出（Simple Custom Detection）] として表示されます。レポートの [詳細（More Details）] セクションのリンクをクリックすると、Secure Endpoint コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。

[高度なマルウェア防御（Secure Endpoint）] レポートページには、新しいセクション、[カテゴリ別受信悪意のあるファイル（Incoming Malicious Files by Category）] があります。このセク

ションには、Secure Endpoint コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブロックリストのファイル SHA の脅威名は、レポートの [悪意のある脅威ファイル（Malicious Threat Files）] セクションに [カスタム検出（Custom Detection）] として表示されます。Secure Endpoint コンソールでブロックリストに登録されたファイル SHA のファイルトラジェクトリの詳細を表示するには、#unique_464を参照してください。

始める前に

Secure Endpoint コンソールの管理アクセス権を伴うユーザーアカウントがあることを確認してください。Secure Endpoint コンソールのユーザーアカウントを作成する方法の詳細については、Cisco TAC にお問い合わせください。

（クラスタ化された設定の場合）クラスタ化された設定では、ログインしているアプライアンスを Secure Endpoint コンソールにのみ登録できます。アプライアンスを Secure Endpoint コンソールにスタンドアロンモードですでに登録している場合は、アプライアンスをクラスタに参加させる前に手動で登録を解除してください。

ファイル レピュテーション フィルタリングが有効化され、設定されていることを確認してください。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「ファイルレピュテーションと分析サービスの有効化と設定」を参照してください。

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 Web インターフェイスの [ファイルレピュテーションとファイル分析（File Reputation and File Analysis）] ページで、[ファイルレピュテーション（File Reputation）] の [詳細設定（Advanced Settings）] パネルにある [Secure Endpointへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックします。

[Secure Endpointへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックすると、 Secure Endpoint コンソールのログインページが表示されます。

ステップ 4 Web インターフェイスの [マルウェア対策レピュテーション（Anti-Malware Reputation）] ページで、[ファイルレピュテーション（File Reputation）] の [詳細設定（Advanced Settings）] パネルにある [Secure Endpoint へのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックします。

[Secure Endpointへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックすると、 Secure Endpoint コンソールのログインページが表示されます。

（注） Secure Endpoint にアプライアンスを登録する前に、ファイル レピュテーション フィルタリングを有効にし、設定する必要があります。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「ファイルレピュテーションと分析サービスの有効化と設定」を参照してください。

ステップ 5 ご使用のユーザーログイン情報で、Secure Endpoint コンソールにログインします。

ステップ 6 Secure Endpoint の認証ページで [許可（Allow）] をクリックして、アプライアンスを登録します。

[許可（Allow）] をクリックすると登録が完了し、アプライアンスの [マルウェア対策レピュテーション（Anti-Malware Reputation）] ページにリダイレクトされます。[Secure Endpoint コンソールの統合（Secure Endpoint AMP for Endpoints Console Integration）] フィールドに、お使いのアプライアンスの名前が表示されます。アプライアンス名は、 Secure Endpoint のコンソールページでアプライアンス設定をカスタマイズする際に使用できます。

次のタスク

次の手順：

- Secure Endpoint コンソールページの [アカウント（Accounts）] > [アプリケーション（Applications）] セクションに移動すると、アプライアンスが Secure Endpoint コンソールに登録されているかどうかを確認できます。アプライアンス名は、 Secure Endpoint コンソールページの [アプリケーション（Applications）] セクションに表示されます。
- 登録されたアプライアンスは、デフォルトのポリシー（ネットワーク ポリシー）が関連付けられたデフォルトのグループ（監査グループ）に追加されます。デフォルトポリシーには、ブロックリストまたは許可リストに追加されるファイル SHA が含まれています。Secure Endpoint の設定をお使いのアプライアンス用にカスタマイズして、ブロックリストまたは許可リストに追加されている独自のファイル SHA を追加する場合は、https://console.amp.cisco.com/docs で Secure Endpoint のユーザーマニュアルを参照してください。
- アプライアンス接続を Secure Endpoint コンソールから登録解除するには、アプライアンスの [ファイルレピュテーション（File Reputation）] セクションの [詳細設定（Advanced Settings）] で [登録解除（Deregister）] をクリックするか、または Secure Endpoint のコンソールページ（https://console.amp.cisco.com/）にアクセスする必要があります。詳細については、https://console.amp.cisco.com/docs で Secure Endpoint のユーザーマニュアルを参照してください。

（注） ファイル レピュテーション サーバーを別のデータセンターに変更すると、アプライアンスは Secure Endpoint コンソールから自動的に登録解除されます。ファイル レピュテーション サーバーに選択された同じデータセンターを使用して、アプライアンスを Secure Endpoint コンソールに再登録する必要があります。

（注） 悪意のあるファイル SHA がクリーンと判定される場合、そのファイル SHA が Secure Endpoint コンソールで許可リストに追加されていないか確認する必要があります。

データベース テーブルの保持

Web レピュテーション、Webroot、Sophos、および McAfee のデータベースは、Cisco アップデート サーバーから定期的にアップデートを受信します。サーバーのアップデートは自動化されており、アップデート間隔はサーバーによって設定されます。

Web レピュテーション データベース

Secure Web Applianceが保持しているフィルタリング データベースには、統計情報およびさまざまなタイプの要求の処理方法に関する情報が含まれています。また、Cisco SensorBase ネットワーク サーバーに Web レピュテーション統計情報を送信するようにアプライアンスを設定することもできます。SensorBase サーバー情報は SensorBase ネットワークからのデータ フィードに活用され、Web レピュテーション スコアの作成に使用されます。

Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング

アクセス ログ ファイルには、Web レピュテーション フィルタと DVS エンジンから返された各トランザクションの情報が記録されます。アクセス ログのスキャン判定情報セクションには、トランザクションに適用されたアクションの原因を把握するのに役立つ多くのフィールドがあります。たとえば、あるフィールドには、Sopho から DVS エンジンに渡された Web レピュテーション スコアやマルウェア スキャン判定が表示されます。

適応型スキャンのロギング

アクセス ログのカスタム フィールド	W3C ログのカスタム フィールド	説明
%X6	x-as-malware-threat-name	適応型スキャンから返されたマルウェア対策名。トランザクションがブロックされていない場合、このフィールドはハイフン（「-」）を返します。この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。

適応型スキャン エンジンによってブロックおよびモニターされるトランザクションは、以下の ACL デシジョン タグを使用します。

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

キャッシング

以下のガイドラインは、AsyncOSがマルウェアのスキャン中にキャッシュを使用する仕組みを示しています。

- AsyncOS は、オブジェクト全体がダウンロードされたときにだけオブジェクトをキャッシュします。スキャン中にマルウェアがブロックされた場合、オブジェクト全体はダウンロードされないので、キャッシュされません。
- AsyncOS は、コンテンツの取得元がサーバーであるか Web キャッシュであるかにかかわらず、コンテンツをスキャンします。
- コンテンツがキャッシュされる時間はさまざまな要因によって異なります。デフォルト値はありません。
- AsyncOS は、シグニチャが更新されるとコンテンツを再スキャンします。

マルウェアのカテゴリについて

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザーがシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザー設定の乗っ取りに関連するさまざまな機能を実行する可能性があるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザーの完全な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザーを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザーの承諾なしにユーザーを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザーのシステムに不要な変更を加えたりします。
悪意のある既知の高リスクファイル	これらは、Secure Endpoint ファイル レピュテーション サービスによって脅威と判定されたファイルです。

マルウェアのタイプ	説明
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
フィッシング URL	フィッシングURLは、ブラウザのアドレスバーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが望ましくないと見なされるアプリケーションです。
システム モニター	システム モニターには、以下のいずれかを実行するソフトウェアが含まれます。 • 公然と、または密かに、システムプロセスやユーザアクションを記録する。 • これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモートホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定のWebページがアクセスされるのを待ったり、感染したマシンをスキャンしてユーザー名とパスフレーズを探したりします。
ウイルス	ウイルスは、ユーザーが気付かない間にコンピュータにロードされるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、悪質なアクションを実行するプログラムまたはアルゴリズムです。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。